AMENDMENTS TO THE CLAIMS:

The following listing of claims will replace all prior versions of claims in the application:

1. (Currently Amended) An apparatus for controlling operations by a client on a ~~stored~~ file stored on a network device, said apparatus comprising:

a first memory associated with the file, said first memory for storing a fixed file security status, said fixed file security status being either of a first type or of a second type, wherein said first type indicates that operations are not allowed on the file and said second type indicates that operations are allowed on the file;

a second memory associated with the file, said second memory for storing an active file security status, said active file security status being either of said first type or of said second type and changeable from said first type to said second type ~~initially copied from said fixed file security status and initially being of said first type and changeable to a second type~~;

~~a request handler receiving a request from the client to perform operations on the file, said request handler disallowing the client from performing operations on the file if said active file security status is of said first type and allowing the client to perform operations on the file if said active file security status is of said second type; and~~

an independent verification routine having access to a security database listing clients and corresponding privileges, ~~and routine is capable of receiving an authorization credential from the client, said independent verification routine causing said active file security status to change to said second type if said authorization credential indicates that the client has the privilege to access the file~~ wherein said independent verification routine is enabled:

to determine whether the client has privilege to perform operations on the file based at least in part on an authorization credential from the client and

to generate either a positive or a negative determination upon request;

and

a request handler in communication with said first memory, said second memory, and said independent verification routine, wherein said request handler is enabled:

to receive a request from the client to open the file;

to transmit a file descriptor to the client;

to copy said fixed file security status from said first memory to said second memory as said active file security status;

to determine whether said active file security status is of said first type or of said second type;

when said active file security status is determined to be of said second type:

to receive a request from the client to perform an operation on the file;

to determine that said active file security status is of said second type; and

to perform the operation requested by the client on the file;

and

when said active file security status is determined to be of said first type:

to receive said authorization credential from the client;

to pass said authorization credential to said independent verification routine;

to receive a positive determination from said independent verification routine that the client has privilege to perform operations on the file;

to change said active file security status from said first type to said second type;

to receive a request from the client to perform an operation on the file;

to determine that said active file security status is of said second type; and

to perform the operation requested by the client on the file.

2. (Previously Presented) The apparatus of claim 1, further comprising a third memory associated with the file, said third memory for storing a delete-on-close status, said delete-on-close status initially set to a first value and changeable to a second value,

wherein said first value indicates that the file will not be deleted upon closing and the second value indicates that the file will be deleted upon closing.

3. (Original) The apparatus of claim 2, wherein said first memory is a non-volatile random-access memory and said second memory and third memory are in a file entry.

4. (Original) The apparatus of claim 3, wherein said first memory, said second memory, and said third memory comprise single bits.

5-26. (Canceled)

27. (New) A method for controlling operations by a client on a file stored on a network device having a first memory associated with the file and a second memory associated with the file, wherein the first memory stores a fixed file security status being either of a first type or of a second type and the second memory stores an active file security status being either of the first type or of the second type and changeable from the first type to the second type and wherein the first type indicates that operations are not allowed on the file and the second type indicates that operations are allowed on the file, the method comprising:

receiving a request from the client to open the file;

transmitting a file descriptor to the client;

copying the fixed file security status from the first memory to the second memory as the active file security status;

determining whether the active file security status is of the first type or of the second type;

when the active file security status is determined to be of the second type:

receiving a request from the client to perform an operation on the file;

determining that the active file security status is of the second type; and

performing the operation requested by the client on the file;

and

when the active file security status is determined to be of the first type:

receiving an authorization credential from the client;

passing the authorization credential to an independent verification routine that determines whether the client has privilege to perform operations on the file;

receiving a positive determination from the independent verification routine that the client has privilege to perform operations on the file;

changing the active file security status from the first type to the second type;

receiving a request from the client to perform an operation on the file;

determining that the active file security status is of the second type; and

performing the operation requested by the client on the file.

28. (New) The method as defined in claim 27, wherein when the active file security status is determined to be of the first type and before changing the active file security status, the method further comprises:

receiving a request from the client to perform an operation on the file; and

returning an error message to the client indicating a refusal to perform the operation requested by the client on the file.

29. (New) The method as defined in claim 27, wherein when the active file security status is determined to be of the first type and after passing the authorization credential, the method further comprises:

receiving a negative determination from the independent verification routine that the client has no privilege to perform operations on the file;

receiving a request from the client to perform an operation on the file; and

returning an error message to the client indicating a refusal to perform the operation requested by the client on the file.

30. (New) An apparatus for controlling operations by a client on a file stored on a network device having a first memory associated with the file and a second memory associated with the file, wherein the first memory stores a fixed file security status being either of a first type or of a second type and the second memory stores an active file security status being either of the first type or of the second type and changeable from the first type to the second type and wherein the first type indicates that operations are not allowed on the file and the second type indicates that operations are allowed on the file, the apparatus comprising:

means for receiving a request from the client to open the file;

means for transmitting a file descriptor to the client;

means for copying the fixed file security status from the first memory to the second memory as the active file security status;

means for determining whether the active file security status is of the first type or of the second type;

when the active file security status is determined to be of the second type:

means for receiving a request from the client to perform an operation on the file;

means for determining that the active file security status is of the second type; and

means for performing the operation requested by the client on the file;

and

when the active file security status is determined to be of the first type:

means for receiving an authorization credential from the client;

means for passing the authorization credential to an independent verification routine that determines whether the client has privilege to perform operations on the file;

means for receiving a positive determination from the independent verification routine that the client has privilege to perform operations on the file;

means for changing the active file security status from the first type to the second type;

means for receiving a request from the client to perform an operation on the file;

means for determining that the active file security status is of the second type; and

means for performing the operation requested by the client on the file.

31. (New) The apparatus as defined in claim 30, wherein when the active file security status is determined to be of the first type and before the active file security status has been changed, the apparatus further comprises:

means for receiving a request from the client to perform an operation on the file; and

means for returning an error message to the client indicating a refusal to perform the operation requested by the client on the file.

32. (New) The apparatus as defined in claim 30, wherein when the active file security status is determined to be of the first type and after the authorization credential has been passed, the apparatus further comprises:

means for receiving a negative determination from the independent verification routine that the client has no privilege to perform operations on the file;

means for receiving a request from the client to perform an operation on the file; and

means for returning an error message to the client indicating a refusal to perform the operation requested by the client on the file.

33. (New) A computer-readable medium having stored thereon computer-executable instructions for performing a method for controlling operations by a client on a file stored on a network device having a first memory associated with the file and a second memory associated with the file, wherein the first memory stores a fixed file security status being either of a first type or of a second type and the second memory stores an active file security status being either of the first type or of the second type and changeable from the first type to the second type and wherein the first type indicates that operations are not allowed on the file and the second type indicates that operations are allowed on the file, the method comprising:

receiving a request from the client to open the file;

transmitting a file descriptor to the client;

copying the fixed file security status from the first memory to the second memory as the active file security status;

determining whether the active file security status is of the first type or of the second type;

when the active file security status is determined to be of the second type:

receiving a request from the client to perform an operation on the file;

determining that the active file security status is of the second type; and

performing the operation requested by the client on the file;

and

when the active file security status is determined to be of the first type:

receiving an authorization credential from the client;

passing the authorization credential to an independent verification routine that determines whether the client has privilege to perform operations on the file;

receiving a positive determination from the independent verification routine that the client has privilege to perform operations on the file;

changing the active file security status from the first type to the second type;

receiving a request from the client to perform an operation on the file;

determining that the active file security status is of the second type; and

performing the operation requested by the client on the file.

34. (New) The computer-readable medium as defined in claim 33, wherein when the active file security status is determined to be of the first type and before changing the active file security status, the method further comprises:

receiving a request from the client to perform an operation on the file; and

returning an error message to the client indicating a refusal to perform the operation requested by the client on the file.

35. (New) The computer-readable medium as defined in claim 33, wherein when the active file security status is determined to be of the first type and after passing the authorization credential, the method further comprises:

receiving a negative determination from the independent verification routine that the client has no privilege to perform operations on the file;

receiving a request from the client to perform an operation on the file; and

returning an error message to the client indicating a refusal to perform the operation requested by the client on the file.